

PR4



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
 United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/883,625	06/18/2001	Jacob Joel Faul	CARDIFF.047A	1239

20995 7590 09/29/2004

KNOBBE MARTENS OLSON & BEAR LLP
 2040 MAIN STREET
 FOURTEENTH FLOOR
 IRVINE, CA 92614

EXAMINER

VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 09/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/883,625

Applicant(s)

FAUL, JACOB JOEL

Examiner

Michael R Vaughan

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 June 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 June 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) *
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2-11-02.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claims 1-23 have been examined and are pending.

Information Disclosure Statement

An initialed and dated copy of Applicant's IDS form 1449, filed 2-11-02, is attached to the instant Office action.

Claim Rejections - 35 USC ' 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the

Art Unit: 2131

requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-3, 14, and 17 are rejected under 35 U.S.C. 102(b) as being anticipated by Merkle (5,157,726).

As per claim 1, Merkle teaches a method of verifying a transaction conducted between a first party and a second party, the method comprising: receiving transaction elements of the transaction; identifying at least a portion of the received transaction elements as selected elements; encrypting the selected elements based on a private key of the first party to generate an encrypted code; printing at least a portion of the received transaction elements on a hard copy transaction certificate; printing the encrypted code on the hard copy transaction certificate; sending the transaction certificate with the encrypted code to the second party; and instructing the second party to scan the transaction certificate to convert the encrypted code to electronic form, and to decrypt the encrypted code in electronic form based on a public key of the first party to generate decrypted selected elements, wherein the decrypted selected elements can be used by the second party to prove the transaction (col. 3, lines 30-60).

As per claim 2, Merkle teaches prompting the second part to enter transaction elements of the transaction on an electronic document (col. 3, line 35) and receiving

Art Unit: 2131

transaction elements comprises receiving transaction entered by the second party on the electronic transaction document (col. 3, lines 64-66).

As per claim 3, Merkle teaches identifying an element of a current date and time (col. 2, line 31).

As per claims 14 and 17 Merkle teaches transmitting transaction elements of the transaction to the first party; receiving a hard copy transaction certificate that includes an encrypted code; scanning the received transaction certificate to convert the encrypted code to electronic form; retrieving a public key of the first party; and decrypting the converted encrypted code based on the retrieved public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction (col. 3, lines 30-60).

Claims 4-5, 15, 18, 20, and 22, are rejected under 35 U.S.C. 102(b) as being anticipated by Haber et al, hereinafter Haber (USP RE. 34, 954).

As per claims 4 and 20, Haber teaches receiving transaction elements of the transaction; identifying at least a portion of the received transaction elements as selected elements; attaching at least a portion of the received transaction elements to a certificate template; encrypting the selected elements based on a private key of the first party to generate an encrypted code; attaching the encrypted code to the certificate

Art Unit: 2131

template to produce a transaction certificate; transmitting the transaction certificate with the encrypted code to the second party (col. 3, lines 3-9); and instructing the second party to decrypt the encrypted code of the transaction certificate based on a public key of the first party to generate decrypted selected elements, wherein the decrypted selected elements can be used by the second party to prove the transaction (col. 4, lines 1-8).

As per claim 5, Haber teaches prompting the second part to enter transaction elements of the transaction on an electronic document and receiving transaction elements comprises receiving transaction entered by the second party on the electronic transaction document (col. 4, line 14).

As per claim 8, Haber teaches identifying an element of a current date and time (col. 4, line 13).

As per claims 15, 18, and 22, Haber teaches transmitting transaction elements of the transaction to the first party; receiving a transaction certificate that includes an encrypted code; retrieving a public key of the first party; and decrypting the included encrypted code based on the retrieved public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction (col. 4, lines 1-8).

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber in view of FAQ published by Stardock: Electronic Store, hereinafter Stardock.

As per claims 6-7, Haber is silent in disclosing that the certificate receipt is sent to the second party via email or that the email contains a URL. Stardock teaching that once a transaction is completed and receipt is email to the second party. In the email, contains an URL to allow the user to quickly access the receipt. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Stardock within the system of Haber because it would allow an

efficient method to return the receipt to the second party whereby he/she can easily obtain the receipt as needed.

Claims 9-10, 13, 16, 19, 21, and 23, are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber in view of Schneier, Applied Cryptography.

As per claims 9 and 21, Haber teaches receiving transaction elements of the transaction; identifying at least a portion of the received transaction elements as selected elements; attaching at least a portion of the received transaction elements to a certificate template; encrypting the selected elements based on a private key of the first party to generate an encrypted code; attaching the encrypted code to the certificate template to produce a transaction certificate; transmitting the transaction certificate with the encrypted code to the second party (col. 3, lines 3-9); and instructing the second party to decrypt the encrypted code of the transaction certificate based on a public key of the first party to generate decrypted selected elements, wherein the decrypted selected elements can be used by the second party to prove the transaction (col. 4, lines 1-8). Haber is silent in disclosing that the first party encrypts the certificate with the public key of the second party after signing the transaction certificate. Schneier teaches signing a certificate and then using the second party's public key to encrypt the certificate before sending it to the second party (pg. 42). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the

teachings of Schneier within the system of Haber because it would encrypt the transaction so allow the second party would be able to reveal its contents.

As per claim 10, Haber teaches prompting the second part to enter transaction elements of the transaction on an electronic document and receiving transaction elements comprises receiving transaction entered by the second party on the electronic transaction document (col. 4, line 14).

As per claim 13, Haber teaches identifying an element of a current date and time (col. 4, line 13).

As per claims 16, 19, and 23, Haber teaches making a public key of the second party available to the first party; transmitting transaction elements of the transaction to the first party; receiving an encrypted transaction certificate; decrypting the received encrypted transaction certificate based on a private key of the second party so as to generate a transaction certificate with an encrypted code; retrieving a public key of the first party; and decrypting the encrypted code based on the retrieved public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to move the transaction (col. 4, lines 1-8). Haber is silent in disclosing that the first party encrypts the certificate with the public key of the second party after signing the transaction certificate. Schneier teaches signing a certificate and then using the second party's public key to encrypt the certificate before sending it to the second party

Art Unit: 2131

(pg. 42). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Schneier within the system of Haber because it would encrypt the transaction so allow the second party would be able to reveal its contents. Decrypting would then follow the necessary protocol of using the public key of the first party to decrypt the receipt to reveal the certificate.

Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber and Schneier as applied to claim 9 above, and further in view of Stardock.

As per claims 11-12, Haber and Schneier are silent in disclosing that the certificate receipt is sent to the second party via email or that the email contains a URL. Stardock teaching that once a transaction is completed and receipt is email to the second party. In the email, contains an URL to allow the user to quickly access the receipt. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Stardock within the system of Haber and Schneier because it would allow an efficient method to return the receipt to the second party whereby he/she can easily obtain the receipt as needed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MV
Michael R Vaughan

Examiner

Art Unit 2131


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100